ROGER WICKER, MISSISSIPPI ROY BUNT, MISSOURI TED CRUZ TEXAS DEB FISCHER, NEBRASKA JERRY MORAN, KANSAS DAN SULLIVAN, ALASKA DEAN HELLER, MEVADA JAMES RINFORE, OKLAHOMA MIKE LEE UTAH RON JOHNSON, WISCONSIN SHELLEY MOORE CAPITO, WEST VIRGINIA CONY GARBINER, COLDRADO

TODD YOUNG, INDIANA

BILL NELSON, FLORIDA
MARIA CANTYVELL, WASHINIGTON
MARIA CANTYVELL, WASHINIGTON
AMY XLOBUCHAR, MINNEGOTA
BICHARD BLUMENTHAL, CONNECTICLT
BRIAN SCHATZ, HAWAJI
EDWARID MARKEY, MASSACHUSETTS
TOM JUDALL, NEW MEXICO
GARY PETERS, MICHIGAN
TAMMY GALDWIN, WISCONSIN
TAMMY GALDWIN, WISCONSIN
MAGGIE HARSSAY, NEW HAMPSHIRE
CATHERINE CORTEZ MASTO, NEVADA
JON TESTER, MONTANA

NICK ROSSI, STAFF DIRECTOR KIM LIPSKY, DEMOCRATIC STAFF DIRECTOR

United States Senate

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEBSITE: http://commerce.senate.gov

February 15, 2018

Mr. Jeffrey P. Bezos President, Chief Executive Officer, and Chairman of the Board Amazon.com, Inc. 410 Terry Avenue North Seattle, WA 98109

Dear Mr. Bezos:

Academic and independent security researchers, ¹ some of whom were federally-funded, ² recently discovered three vulnerabilities in modern computer processers that have existed for more than two decades. ³ These side-channel vulnerabilities, ⁴ which researchers have named "Meltdown" and "Spectre," could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information. ⁵

¹ Affiliated with Google's Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.

² Nat'l Instl of Standards and Tech., "70NANB15H328, Provable Security for Next-Generation Cryptography;" Nat'l Sci. Found., "Award 1514261, TWC: Medium: Apollo: An Architecture for Scalable Verifiable Computing;" and Nat'l Sci. Found., "Award 1652259, CAREER: Towards Practical Systems for Trustworthy Cloud Computing."
³ Horn, Jann, "Reading Privileged Memory with a Side-Channel," January 3, 2018; Kocher, Paul, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom, "Spectre Attacks: Exploiting Speculative Execution," January 03, 2018; Lipp, Moritz, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg, "Meltdown," January 03, 2018; Galowicz, Jacek, Cyberus Technology, "Meltdown," January 3, 2018.

⁴ Nat'l Inst. of Standards and Tech., Nat'l Vulnerability Database, "CVE-2017-5754 Detail," "CVE-2017-5733 Detail," and "CVE-2017-5715 Detail," January 4, 2018.

⁵ "Alert (TA 1804A): Meltdown and Spectre Side-Channel Vulnerability Guidance," January 4, 2018, https://www.us-cert.gov/ncas/alerts/TA18-004A.

⁶ Busvine, Douglas, and Stephen Nellis, "Security Flaws Put Virtually All Phones, Computers at Risk," January 04, 2018, Accessed January 31, 2018, https://www.reuters.com/article/us-cyber-intel/security-flaws-put-virtually-all-phones-computers-at-risk-idUSKBN1ES1BO.

Mr. Jeffrey P. Bezos February 15, 2018 Page 2 of 3

International Organization for Standardization (ISO).⁷ These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face.⁸ They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry's coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

- 1. When and how did you first become aware of these vulnerabilities?
- 2. Which of your products are affected by these vulnerabilities and how are they affected?
- 3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

Nat'l Inst. of Standards and Tech., Computer Security Resource Center, "Non-Invasive Attack Testing Workshop," Updated August 17, 2011, available at: https://csrc.nist.gov/Events/2011/Non-Invasive-Attack-Testing-Workshop; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/52906.html; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/60612.html

8 Schneier, Bruce, "The New Way Your Computer Can Be Attacked," *The Atlantic*, January 22, 2018, accessed February 01, 2018, https://www.theatlantic.com/technology/archive/2018/01/spectre-meltdown-cybersecurity/551147/.

⁹ Newman, Lily Hay, "Meltdown and Spectre Patching has been a Total Train Wreck," *Wired*, January 23, 2018, accessed February 1, 2018, https://www.wired.com/story/meltdown-spectre-patching-total-train-wreck/

¹⁰ McMillan, Robert, and Liza Lin, "Intel Warned Chinese Companies of Chip Flaws before U.S. Government," January 28, 2018, accessed February 1, 2018, https://www.wsj.com/articles/intel-warned-chinese-companies-of-chip-flaws-before-u-s-government-1517157430

- 4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?
- 5. What steps have you taken to mitigate or patch these vulnerabilities?
- 6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?
- 7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.
- 8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?
- 9. To what degree are you coordinating your response with other companies?
- 10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

Sincerely,

JOHN THUNE Chairman

BILL NELSON Ranking Member

L Nelson

ROGER WICKER, MISSISSIPPI ROY BUUNT, MISCOURI TED CRUZ, TEXAS DEB FISCHER, NEBRASKA DEB FISCHER, NEBRASKA DER SIECHWAN, ALASKA DEAN HELLER, NEWADA JAMES INNOED CINCLAHOMA MIKE LEE, UTAH RON JUNKON, WISCONSIN SIN JUNKON, WISCONSIN BILI NELSON, FLORIDA
MARIA CANTWELL, WASHINGTON
AMY KLOBUCHAR, MININESOTA
RICHARD BLUMENTHAL CONNECTICUT
BRIAN SCHATZ, HAWAII
EDWARD MARKEY, MASSACHUSETTS
TOM IDALL, NEW MEXICO
GARY PETERS, MICHIGAN
TAMMY BALDWIN, WISCONSIN
TAMMY DUCKWORTH, ILLINGIS
MAGGIE HASSAN, NEW HAMPSHIRE
CATHERINE CORTEZ MASTO, NEVADA
KINSTESTER MONTANA

NICK HOSSI, STAFF DIRECTOR KIM LIPSKY DEMOCRATIC STAFF DIRECTOR

United States Senate

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEBSITE: http://commerce.senate.gov

February 15, 2018

Mr. Tim Cook Chief Executive Officer Apple Inc. 1 Infinite Loop Cupertino, CA 95014

Dear Mr. Cook:

Academic and independent security researchers, ¹ some of whom were federally-funded, ² recently discovered three vulnerabilities in modern computer processers that have existed for more than two decades. ³ These side-channel vulnerabilities, ⁴ which researchers have named "Meltdown" and "Spectre," could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information. ⁵

According to one of the researchers, the Meltdown vulnerability is "probably one of the worst CPU [central processing unit] bugs ever found," while Spectre, although arguably more difficult to exploit, presents more significant challenges to mitigate or patch. For years, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has been concerned with such side-channel attacks and their impact on cryptography. In 2011, NIST held a testing workshop and coauthored standards in cooperation and accordance with the

¹ Affiliated with Google's Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.

² Nat'l Instl of Standards and Tech., "70NANB15H328, Provable Security for Next-Generation Cryptography;" Nat'l Sci. Found., "Award 1514261, TWC: Medium: Apollo: An Architecture for Scalable Verifiable Computing," and Nat'l Sci. Found., "Award 1652259, CAREER: Towards Practical Systems for Trustworthy Cloud Computing." ³ Horn, Jann, "Reading Privileged Memory with a Side-Channel," January 3, 2018; Kocher, Paul, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom, "Spectre Attacks: Exploiting Speculative Execution," January 03, 2018; Lipp, Moritz, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg, "Meltdown," January 03, 2018; Galowicz, Jacek, Cyberus Technology, "Meltdown," January 3, 2018.

⁴ Nat'l Inst. of Standards and Tech., Nat'l Vulnerability Database, "CVE-2017-5754 Detail," "CVE-2017-5733 Detail," and "CVE-2017-5715 Detail," January 4, 2018.

⁵ "Alert (TA 1804A): Meltdown and Spectre Side-Channel Vulnerability Guidance," January 4, 2018, https://www.us-cert.gov/ncas/alerts/TA18-004A.

⁶ Busvine, Douglas, and Stephen Nellis, "Security Flaws Put Virtually All Phones, Computers at Risk," January 04, 2018, Accessed January 31, 2018, https://www.reuters.com/article/us-cyber-intel/security-flaws-put-virtually-all-phones-computers-at-risk-idUSKBN1ES1BO.

Mr. Tim Cook February 15, 2018 Page 2 of 3

International Organization for Standardization (ISO).⁷ These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face.⁸ They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry's coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

- 1. When and how did you first become aware of these vulnerabilities?
- 2. Which of your products are affected by these vulnerabilities and how are they affected?
- 3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

⁷ Nat'l Inst. of Standards and Tech., Computer Security Resource Center, "Non-Invasive Attack Testing Workshop," Updated August 17, 2011, available at: https://csrc.nist.gov/Events/2011/Non-Invasive-Attack-Testing-Workshop; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/52906.html; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/60612.html

8 Schneier, Brüce, "The New Way Your Computer Can Be Attacked," *The Atlantic*, January 22, 2018, accessed February 01, 2018, https://www.theatlantic.com/technology/archive/2018/01/spectre-meltdown-cybersecurity/551147/.

Newman, Lily Hay, "Meltdown and Spectre Patching has been a Total Train Wreck," Wired, January 23, 2018, accessed February 1, 2018, https://www.wired.com/story/meltdown-spectre-patching-total-train-wreck/
 McMillan, Robert, and Liza Lin, "Intel Warned Chinese Companies of Chip Flaws before U.S. Government," January 28, 2018, accessed February 1, 2018, https://www.wsj.com/articles/intel-warned-chinese-companies-of-chip-flaws-before-u-s-government-1517157430

- 4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?
- 5. What steps have you taken to mitigate or patch these vulnerabilities?
- 6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?
- 7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.
- 8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?
- 9. To what degree are you coordinating your response with other companies?
- 10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

Sincerely,

JOHN THUNE

Chairman

BILL NELSON Ranking Member

U Nelson

ROGER WICKER, MISSISSIPPI ROY BLUNT, MISSOURI TED CRUZ, TEXAS DER FISCHER, NEBRASKA JERRY MORAN, KANSAS DAN SULLIYAN, ALASKA DEAN HELLER, NEVADA JAMES INHOFE, OKLAHOMA MIKE LEE, UTAH ROUSEN JOHNSON, WISCONSIN SHELLEY MOCHE CAPITO, WEST VIRG CORY GARDNER, COLOHADO TODO YOUNG! MOIANA

BILL NELSON, FLORIDA
MARIA CANTWELL, WASHINGTON
MARIA CANTWELL, WASHINGTON
RICHARD BLUMENTHAL CONNECTICUT
BERIAN SCHATZ, HAWAII
EDWARD MARKEY, MASSACHUSETTS
TOM UDALL, NEW MEXICO
GARY FETERS, MICHIGAN
TAMMY DUCKWORTH, ILLINOIS
MAGGIE HASSAN, NEW HAMPSHIRE
CATHERINE CORTEZ MASTO, NEVADA

NICK ROSSI STAFF DIRECTOR KIM LIPSKY, DEMICRATIC STAFF DIRECTOR

United States Senate

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEBSITE: http://commerce.senate.gov

February 15, 2018

Mr. Jensen Huang President and Chief Executive Officer NVIDIA Corporation 2788 San Tomas Expressway Santa Clara, CA 95051

Dear Mr. Huang:

Academic and independent security researchers, ¹ some of whom were federally-funded, ² recently discovered three vulnerabilities in modern computer processers that have existed for more than two decades. ³ These side-channel vulnerabilities, ⁴ which researchers have named "Meltdown" and "Spectre," could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information. ⁵

¹ Affiliated with Google's Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.

² Nat'l Instl of Standards and Tech., "70NANB15H328, Provable Security for Next-Generation Cryptography;" Nat'l Sci. Found., "Award 1514261, TWC: Medium: Apollo: An Architecture for Scalable Verifiable Computing;" and Nat'l Sci. Found., "Award 1652259, CAREER: Towards Practical Systems for Trustworthy Cloud Computing." ³ Horn, Jann, "Reading Privileged Memory with a Side-Channel," January 3, 2018; Kocher, Paul, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom, "Spectre Attacks: Exploiting Speculative Execution," January 03, 2018; Lipp, Moritz, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg, "Meltdown," January 03, 2018; Galowicz, Jacek, Cyberus Technology, "Meltdown," January 3, 2018.

⁴ Nat'l Inst. of Standards and Tech., Nat'l Vulnerability Database, "CVE-2017-5754 Detail," "CVE-2017-5733 Detail," and "CVE-2017-5715 Detail," January 4, 2018.

⁵ "Alert (TA 1804A): Meltdown and Spectre Side-Channel Vulnerability Guidance," January 4, 2018, https://www.us-cert.gov/ncas/alerts/TA18-004A.

⁶ Busvine, Douglas, and Stephen Nellis, "Security Flaws Put Virtually All Phones, Computers at Risk," January 04, 2018, Accessed January 31, 2018, https://www.reuters.com/article/us-cyber-intel/security-flaws-put-virtually-all-phones-computers-at-risk-idUSKBN1ES1BO.

Mr. Jensen Huang February 15, 2018 Page 2 of 3

International Organization for Standardization (ISO).⁷ These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face.⁸ They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry's coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

- 1. When and how did you first become aware of these vulnerabilities?
- 2. Which of your products are affected by these vulnerabilities and how are they affected?
- 3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

⁷ Nat'l Inst. of Standards and Tech., Computer Security Resource Center, "Non-Invasive Attack Testing Workshop," Updated August 17, 2011, available at: https://csrc.nist.gov/Events/2011/Non-Invasive-Attack-Testing-Workshop; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/52906.html; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/60612.html

Schneier, Bruce, "The New Way Your Computer Can Be Attacked," *The Atlantic*, January 22, 2018, accessed February 01, 2018, https://www.theatlantic.com/technology/archive/2018/01/spectre-meltdown-cybersecurity/551147/.

⁹ Newman, Lify Hay, "Meltdown and Spectre Patching has been a Total Train Wreck," Wired, January 23, 2018, accessed February 1, 2018, https://www.wired.com/story/meltdown-spectre-patching-total-train-wreck/

¹⁰ McMillan, Robert, and Liza Lin, "Intel Warned Chinese Companies of Chip Flaws before U.S. Government," January 28, 2018, accessed February 1, 2018, https://www.wsj.com/articles/intel-warned-chinese-companies-of-chip-flaws-before-u-s-government-1517157430

- 4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?
- 5. What steps have you taken to mitigate or patch these vulnerabilities?
- 6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?
- 7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.
- 8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?
- 9. To what degree are you coordinating your response with other companies?
- 10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

Sincerely,

JOHN THUNE

Chairman

BILL NELSON
Ranking Member

ROGER WICKER, MISSISSIPPI ROY BILLOTI, MISSOURI TED CRILZ, TEXAS DEB FISCHER, NEBRASKA DEB FISCHER, NEBRASKA DEAN HELLER, NEWADA JAMES MINDER DELAHOMA MIKE LEE, UTAH ROMES MINDER DELAHOMA MIKE LEE, UTAH ROMORE CAPITO, WEST VIRGINIA CORY GARDINER, COLORADO BILL NELSON, FLORIDA
MARIA CANTWELL, WASHINGTON
AMY SLOBUCHAR, MINNESOTA
RICHARD BLUMENTHAL, CONNECTICUT
BRIAN SCHATZ, HAWAII
EDWARD MARKEY, MASSACHUSETTS
TOM UDALL, NEW MEXICO
GARV PETERS, MICHIGAN
TAMMY PALDWIN, WISCONSIN
TAMMY DUCKWORTH, ILLINOIS
MAGGIE HASSAN, NEW HAMPSHIRF
CATHERINE COFTEZ MAGTO, NEVADA
JON TESTER, MONTANA

NICK ROSSI, STAFF DIRECTOR

United States Senate

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEBSITE: http://commerce.senate.gov

February 15, 2018

Mr. Brian M. Krzanich Chief Executive Officer Intel Corporation 2200 Mission College Boulevard Santa Clara, CA 95054

Dear Mr. Krzanich:

Academic and independent security researchers, ¹ some of whom were federally-funded, ² recently discovered three vulnerabilities in modern computer processers that have existed for more than two decades. ³ These side-channel vulnerabilities, ⁴ which researchers have named "Meltdown" and "Spectre," could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information. ⁵

¹ Affiliated with Google's Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.

² Nat'l Instl of Standards and Tech., "70NANB15H328, Provable Security for Next-Generation Cryptography;" Nat'l Sci. Found., "Award 1514261, TWC: Medium: Apollo: An Architecture for Scalable Verifiable Computing;" and Nat'l Sci. Found., "Award 1652259, CAREER: Towards Practical Systems for Trustworthy Cloud Computing." ³ Horn, Jann, "Reading Privileged Memory with a Side-Channel," January 3, 2018; Kocher, Paul, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom, "Spectre Attacks: Exploiting Speculative Execution," January 03, 2018; Lipp, Moritz, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg, "Meltdown," January 03, 2018; Galowicz, Jacek, Cyberus Technology, "Meltdown," January 3, 2018.

⁴ Nat'l Inst. of Standards and Tech., Nat'l Vulnerability Database, "CVE-2017-5754 Detail," "CVE-2017-5733 Detail," and "CVE-2017-5715 Detail," January 4, 2018.

⁵ "Alert (TA 1804A): Meltdown and Spectre Side-Channel Vulnerability Guidance," January 4, 2018, https://www.us-cert.gov/ncas/alerts/TA18-004A.

⁶ Busvine, Douglas, and Stephen Nellis, "Security Flaws Put Virtually All Phones, Computers at Risk," January 04, 2018, Accessed January 31, 2018, https://www.reuters.com/article/us-cyber-intel/security-flaws-put-virtually-all-phones-computers-at-risk-idUSKBN1ES1BO.

Mr. Brian M. Krzanich February 15, 2018 Page 2 of 3

International Organization for Standardization (ISO).⁷ These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face.⁸ They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry's coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. ¹⁰ As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

- 1. When and how did you first become aware of these vulnerabilities?
- 2. Which of your products are affected by these vulnerabilities and how are they affected?
- 3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

Nat'l Inst. of Standards and Tech., Computer Security Resource Center, "Non-Invasive Attack Testing Workshop," Updated August 17, 2011, available at: https://csrc.nist.gov/Events/2011/Non-Invasive-Attack-Testing-Workshop; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/52906.html; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/60612.html 8 Schneier, Bruce, "The New Way Your Computer Can Be Attacked," *The Atlantic*, January 22, 2018, accessed February 01, 2018, https://www.theatlantic.com/technology/archive/2018/01/spectre-meltdown-cybersecurity/551147/.

Newman, Lily Hay, "Meltdown and Spectre Patching has been a Total Train Wreck," Wired, January 23, 2018, accessed February 1, 2018, https://www.wired.com/story/meltdown-spectre-patching-total-train-wreck/
 McMillan, Robert, and Liza Lin, "Intel Warned Chinese Companies of Chip Flaws before U.S. Government," January 28, 2018, accessed February 1, 2018, https://www.wsj.com/articles/intel-warned-chinese-companies-of-chip-flaws-before-u-s-government-1517157430

- 4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?
- 5. What steps have you taken to mitigate or patch these vulnerabilities?
- 6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?
- 7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.
- 8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?
- 9. To what degree are you coordinating your response with other companies?
- 10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

Sincerely,

JOHN THUNE

Chairman

BILL NELSON Ranking Member

L Nelson

ROGER WICKER, MISSISSIPPI ROY BLUNT, MISSOURI TED CRUZ TEXAS DEB FISCHER, NEBRASKA JERRY MORAN, KANSAS DAN SULLIVAN, ALASKA DEAN HELLER, NEWADA JAMESI MINDER, OKCAHOMA MIRE LEE, UTAH RON JOHNSON, WISCONSIN SHELLEY MOORE CAPTO, WEST VIRGINIA CORY GARDNER, COLORADO TODO YOUNG, INDIANA

BIL NELSON, FLORIDA
MARIA CANTWELL, WASHINGTON
MARIA CANTWELL, WASHINGTON
ANY KLEBUCHAR, MINNESOTA
RICHARD BLUMENTHAL, CONNECTICUT
BRIAN SCHATZ, HAWAII
EDWARD MARKEY, MASSACHUSETTS
TOM UDALL, NEW MENICO
GARY PETERS, MICHIGAN
TAMMY BALDWIN, WISCONSIN
TAMMY BALDWIN, WISCONSIN
TAMMY DUCKWORTH, ILLINDIS
MAGGIE HASSAN, NEW HAMPSHIRE
CATHERINE CORTEZ MASTO, REVADA
JON TESTER, MONTANA

NICK ROSSI, STAFF DIRECTOR
KIM LIPSKY, DEMOCRATIC STAFF DIRECTOR

United States Senate

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEBSITE: http://commerce.senate.gov

February 15, 2018

Mr. Satya Nadella Chief Executive Officer Microsoft Corporation One Microsoft Way Redmond, WA 98052

Dear Mr. Nadella:

Academic and independent security researchers, ¹ some of whom were federally-funded, ² recently discovered three vulnerabilities in modern computer processers that have existed for more than two decades. ³ These side-channel vulnerabilities, ⁴ which researchers have named "Meltdown" and "Spectre," could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information. ⁵

According to one of the researchers, the Meltdown vulnerability is "probably one of the worst CPU [central processing unit] bugs ever found," while Spectre, although arguably more difficult to exploit, presents more significant challenges to mitigate or patch. For years, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has been concerned with such side-channel attacks and their impact on cryptography. In 2011, NIST held a testing workshop and coauthored standards in cooperation and accordance with the

¹ Affiliated with Google's Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.

² Nat'l Instl of Standards and Tech., "70NANB15H328, Provable Security for Next-Generation Cryptography;" Nat'l Sci. Found., "Award 1514261, TWC: Medium: Apollo: An Architecture for Scalable Verifiable Computing;" and Nat'l Sci. Found., "Award 1652259, CAREER: Towards Practical Systems for Trustworthy Cloud Computing." ³ Horn, Jann, "Reading Privileged Memory with a Side-Channel," January 3, 2018; Kocher, Paul, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom, "Spectre Attacks: Exploiting Speculative Execution," January 03, 2018; Lipp, Moritz, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg, "Meltdown," January 03, 2018; Galowicz, Jacek, Cyberus Technology, "Meltdown," January 3, 2018.

⁴ Nat'l Inst. of Standards and Tech., Nat'l Vulnerability Database, "CVE-2017-5754 Detail," "CVE-2017-5733 Detail," and "CVE-2017-5715 Detail," January 4, 2018.

⁵ "Alert (TA 1804A): Meltdown and Spectre Side-Channel Vulnerability Guidance," January 4, 2018, https://www.us-cert.gov/ncas/alerts/TA18-004A.

⁶ Busvine, Douglas, and Stephen Nellis, "Security Flaws Put Virtually All Phones, Computers at Risk," January 04, 2018, Accessed January 31, 2018, https://www.reuters.com/article/us-cyber-intel/security-flaws-put-virtually-all-phones-computers-at-risk-idUSKBN1ES1BO.

Mr. Satya Nadella February 15, 2018 Page 2 of 3

International Organization for Standardization (ISO).⁷ These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face.⁸ They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry's coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

- 1. When and how did you first become aware of these vulnerabilities?
- 2. Which of your products are affected by these vulnerabilities and how are they affected?
- 3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

⁷ Nat'l Inst. of Standards and Tech., Computer Security Resource Center, "Non-Invasive Attack Testing Workshop," Updated August 17, 2011, available at: https://csrc.nist.gov/Events/2011/Non-Invasive-Attack-Testing-Workshop; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/52906.html; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/60612.html

Schneier, Bruce, "The New Way Your Computer Can Be Attacked," *The Atlantic*, January 22, 2018, accessed February 01, 2018, https://www.theatlantic.com/technology/archive/2018/01/spectre-meltdown-cybersecurity/551147/.

⁹ Newman, Lily Hay, "Meltdown and Spectre Patching has been a Total Train Wreck," Wired, January 23, 2018, accessed February 1, 2018, https://www.wired.com/story/meltdown-spectre-patching-total-train-wreck/
¹⁰ McMillan, Robert, and Liza Lin, "Intel Warned Chinese Companies of Chip Flaws before U.S. Government," January 28, 2018, accessed February 1, 2018, https://www.wsj.com/articles/intel-warned-chinese-companies-of-chip-flaws-before-u-s-government-1517157430

- 4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?
- 5. What steps have you taken to mitigate or patch these vulnerabilities?
- 6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?
- 7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.
- 8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?
- 9. To what degree are you coordinating your response with other companies?
- 10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

Sincerely,

JOHN THUNE

Chairman

L Nelson Ranking Member

ROGER WICKER, MISSISSIPPI ROY BLUNT, MISSOURI TED CRUZ, TEXAS DEB FISCHER, NEBRASKA JERRY MORBAN, KANSAS DAN SULLIVAN, ALASKA DEAN HELCER, NEVADA JAMES INHIPE, DIKLAHOMA MIKE LEE, UTAK ROM JUPINSON, WISCONSIN SHELLEY MOORE CAPITO, WEST VIRGINIA CORY GARDNER, COLORADO TODD YOUNG, MOIL BILL NELSON, FLORIDA
MARIA CANTWELL WASHINGTON
AMY KLOBUCHAR, MINNESOTA
RICHARD BLUMENTHAL, CONNECTICUT
BRIAN SCHAFT, HAWAII
EDWARD MARKEY, MASSACHUSETTS
TOM UDALL, NEW MEXICO
GAPY PETERS, MICHIGAN
TAMMY BALDWIN, WISCONSIN
TAMMY DUCKWORTH, ILUNOIS
MAGGIE HASSAN, NEW HAMPSHIRE
CATHERINE COPTEZ MASTO, NEVADA
LION TESTER MANTANA

NICK ROSSI, STAFF DIRECTOR
KIM LIPSKY, DEMOCRATIC STAFF DIRECTOR

United States Senate

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEBSITE: http://commerce.senate.gov

February 15, 2018

Mr. Sundar Pichai Chief Executive Officer Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043

Dear Mr. Pichai:

Academic and independent security researchers, some of whom were federally-funded, recently discovered three vulnerabilities in modern computer processers that have existed for more than two decades. These side-channel vulnerabilities, which researchers have named "Meltdown" and "Spectre," could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information.

¹ Affiliated with Google's Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.

² Nat'l Instl of Standards and Tech., "70NANB15H328, Provable Security for Next-Generation Cryptography;" Nat'l Sci. Found., "Award 1514261, TWC: Medium: Apollo: An Architecture for Scalable Verifiable Computing," and Nat'l Sci. Found., "Award 1652259, CAREER: Towards Practical Systems for Trustworthy Cloud Computing." ³ Horn, Jann, "Reading Privileged Memory with a Side-Channel," January 3, 2018; Kocher, Paul, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom, "Spectre Attacks: Exploiting Speculative Execution," January 03, 2018; Lipp, Moritz, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg, "Meltdown," January 03, 2018; Galowicz, Jacek, Cyberus Technology, "Meltdown," January 3, 2018.

⁴ Nat'l Inst. of Standards and Tech., Nat'l Vulnerability Database, "CVE-2017-5754 Detail," "CVE-2017-5733 Detail," and "CVE-2017-5715 Detail," January 4, 2018.

⁵ "Alert (TA 1804A): Meltdown and Spectre Side-Channel Vulnerability Guidance," January 4, 2018, https://www.us-cert.gov/ncas/alerts/TA18-004A.

⁶ Busvine, Douglas, and Stephen Nellis, "Security Flaws Put Virtually All Phones, Computers at Risk," January 04, 2018, Accessed January 31, 2018, https://www.reuters.com/article/us-cyber-intel/security-flaws-put-virtually-all-phones-computers-at-risk-idUSKBN1ES1BO.

Mr. Sundar Pichai February 15, 2018 Page 2 of 3

International Organization for Standardization (ISO).⁷ These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face.⁸ They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry's coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

- 1. When and how did you first become aware of these vulnerabilities?
- 2. Which of your products are affected by these vulnerabilities and how are they affected?
- 3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

⁷ Nat'l Inst. of Standards and Tech., Computer Security Resource Center, "Non-Invasive Attack Testing Workshop," Updated August 17, 2011, available at: https://csrc.nist.gov/Events/2011/Non-Invasive-Attack-Testing-Workshop; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/52906.html; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/60612.html
⁸ Schneier, Bruce, "The New Way Your Computer Can Be Attacked," *The Atlantic*, January 22, 2018, accessed February 01, 2018, https://www.theatlantic.com/technology/archive/2018/01/spectre-meltdown-cybersecurity/551147/.

⁹ Newman, Lily Hay, "Meltdown and Spectre Patching has been a Total Train Wreck," Wired, January 23, 2018, accessed February 1, 2018, https://www.wired.com/story/meltdown-spectre-patching-total-train-wreck/
¹⁰ McMillan, Robert, and Liza Lin, "Intel Warned Chinese Companies of Chip Flaws before U.S. Government," January 28, 2018, accessed February 1, 2018, https://www.wsj.com/articles/intel-warned-chinese-companies-of-chip-flaws-before-u-s-government-1517157430

- 4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?
- 5. What steps have you taken to mitigate or patch these vulnerabilities?
- 6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?
- 7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.
- 8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?
- 9. To what degree are you coordinating your response with other companies?
- 10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

Sincerely,

JOHN THUNE

Chairman

BILL NELSON Ranking Member

Nelson

ROGER WICKER, MISSISSIPPI ROY BLUNT, MISSIDIRI TEXAS DEB FISCHER, NEBRASKA JERRY MODRAN, KANSAS DAN SULLIWAN, ALASKA DEAN-HELLER, NEVADA JAMES IRHOPE, DKLAHOMA MIKE LEE, UTAH ROM JOHNSON, WISCONSIN SHELLEY MOORE CAPITO, WIST VIRGINIA CORY GARDONER, ODJORADO

TOOD YOUNG, INDIANA

BILL NELSON, FLORIDA
MARIA CANTWELL, WASHINGTON
AMY KLOBUCHAR, MINNESOTA
RICHARD BLUMENTHAL, CONNECTICUT
BRIAN SCHATZ, SHAWAII
EDWARD MARKEY, MASSACHUSEFTS
TOM
GAMY PETERS, MICHIGAN
TAMMY DUKWORTH, ILLINOIS
MAGGIE HASSAN, NEW HAMPSHIRE
CATHERINE CORTEZ MASTO, NEVADA
JON TESTER, MICHIGAN

NICK ROSSI, STAFF DIRECTOR
KIM LIPSKY, DEMOCRATIC STAFF DIRECTOR

United States Senate

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEBSITE: http://commerce.senate.gov

February 15, 2018

Mr. Chuck Robbins Chairman and Chief Executive Officer Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134

Dear Mr. Robbins:

Academic and independent security researchers, ¹ some of whom were federally-funded, ² recently discovered three vulnerabilities in modern computer processers that have existed for more than two decades. ³ These side-channel vulnerabilities, ⁴ which researchers have named "Meltdown" and "Spectre," could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information. ⁵

¹ Affiliated with Google's Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.

² Nat'l Instl of Standards and Tech., "70NANB15H328, Provable Security for Next-Generation Cryptography;" Nat'l Sci. Found., "Award 1514261, TWC: Medium: Apollo: An Architecture for Scalable Verifiable Computing;" and Nat'l Sci. Found., "Award 1652259, CAREER: Towards Practical Systems for Trustworthy Cloud Computing." ³ Horn, Jann, "Reading Privileged Memory with a Side-Channel," January 3, 2018; Kocher, Paul, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom, "Spectre Attacks: Exploiting Speculative Execution," January 03, 2018; Lipp, Moritz, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg, "Meltdown," January 03, 2018; Galowicz, Jacek, Cyberus Technology, "Meltdown," January 3, 2018.

⁴ Nat'l Inst. of Standards and Tech., Nat'l Vulnerability Database, "CVE-2017-5754 Detail," "CVE-2017-5733 Detail," and "CVE-2017-5715 Detail," January 4, 2018.

⁵ "Alert (TA 1804A): Meltdown and Spectre Side-Channel Vulnerability Guidance," January 4, 2018, https://www.us-cert.gov/ncas/alerts/TA18-004A.

⁶ Busvine, Douglas, and Stephen Nellis, "Security Flaws Put Virtually All Phones, Computers at Risk," January 04, 2018, Accessed January 31, 2018, https://www.reuters.com/article/us-cyber-intel/security-flaws-put-virtually-all-phones-computers-at-risk-idUSKBN1ES1BO.

Mr. Chuck Robbins February 15, 2018 Page 2 of 3

International Organization for Standardization (ISO).⁷ These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face.⁸ They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry's coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

- 1. When and how did you first become aware of these vulnerabilities?
- 2. Which of your products are affected by these vulnerabilities and how are they affected?
- 3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

⁷ Nat'l Inst. of Standards and Tech., Computer Security Resource Center, "Non-Invasive Attack Testing Workshop," Updated August 17, 2011, available at: https://csrc.nist.gov/Events/2011/Non-Invasive-Attack-Testing-Workshop; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/52906.html; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/60612.html

8 Schneier, Bruce, "The New Way Your Computer Can Be Attacked," *The Atlantic*, January 22, 2018, accessed February 01, 2018, https://www.theatlantic.com/technology/archive/2018/01/spectre-melidown-cybersecurity/551147/.

⁹ Newman, Lily Hay, "Meltdown and Spectre Patching has been a Total Train Wreck," *Wired*, January 23, 2018, accessed February 1, 2018, https://www.wired.com/story/meltdown-spectre-patching-total-train-wreck/

¹⁰ McMillan, Robert, and Liza Lin, "Intel Warned Chinese Companies of Chip Flaws before U.S. Government," January 28, 2018, accessed February 1, 2018, https://www.wsj.com/articles/intel-warned-chinese-companies-of-chip-flaws-before-u-s-government-1517157430

- 4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?
- 5. What steps have you taken to mitigate or patch these vulnerabilities?
- 6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?
- 7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.
- 8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?
- 9. To what degree are you coordinating your response with other companies?
- 10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

Sincerely,

JOHN THUNE

Chairman

BILL NELSON Ranking Member

- Nelson

RÖGER WICKER, MISSISSIPPI ROY BLLINT, MISSOURI TED CRUZ, TEXAS DER PISCHER, NEBRASKA JERRY MORAN, KANSAS DAN SULLIVAN, ALASKA DEAN HELLER, NEWADA JAMES INHOTE DIKLAHOMA MIKE LEE, UTAH RON JOHNSON, WISCONSIN SHELLEY MÖDRE CAPITO, WEST VIRGINIA CORY GARDINER, COLDRADO TODO YOUNG, INDIANA BILL NELSON, FLORIDA
MARIA CARTYVELL WASHINGTON
AMY KLOBUCHAR, MINNESOTA
RICHARD BLUMEN THAL, CONNECTICUT
BRIAN SCHATZ, HAWAII
SCHATZ, HAWAII
TON MUDALL, NEW MEXICO
GARY PETERS, MICHEGAN
TAMMY BALDWIN, WISCONSIN
TAMMY DUCKWORTH, ILLINOIS
MAGGIE HASSAN, NEW HAMPSHIRE
CATHERINE CORTEZ MASTO, NEVADA

NICK ROSSI, STAFF DIRECTOR KIM LIPSKY, DEMOCRATIC STAFF DIRECTOR

United States Senate

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEBSITE: http://commerce.senate.gov

February 15, 2018

Ms. Virginia M. Rometty Chairman, President, and Chief Executive Officer International Business Machines Corporation 1 New Orchard Road Armonk, NY 10504

Dear Ms. Rometty:

Academic and independent security researchers, 1 some of whom were federally-funded, 2 recently discovered three vulnerabilities in modern computer processers that have existed for more than two decades. 3 These side-channel vulnerabilities, 4 which researchers have named "Meltdown" and "Spectre," could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information. 5

¹ Affiliated with Google's Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.

² Nat'l Instl of Standards and Tech., "70NANB15H328, Provable Security for Next-Generation Cryptography;" Nat'l Sci. Found., "Award 1514261, TWC: Medium: Apollo: An Architecture for Scalable Verifiable Computing;" and Nat'l Sci. Found., "Award 1652259, CAREER: Towards Practical Systems for Trustworthy Cloud Computing." ³ Horn, Jann, "Reading Privileged Memory with a Side-Channel," January 3, 2018; Kocher, Paul, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom, "Spectre Attacks: Exploiting Speculative Execution," January 03, 2018; Lipp, Moritz, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg, "Meltdown," January 03, 2018; Galowicz, Jacek, Cyberus Technology, "Meltdown," January 3, 2018.

⁴ Nat'l Inst. of Standards and Tech., Nat'l Vulnerability Database, "CVE-2017-5754 Detail," "CVE-2017-5733 Detail," and "CVE-2017-5715 Detail," January 4, 2018.

⁵ "Alert (TA 1804A): Meltdown and Spectre Side-Channel Vulnerability Guidance," January 4, 2018, https://www.us-cert.gov/ncas/alerts/TA18-004A.

⁶ Busvine, Douglas, and Stephen Nellis, "Security Flaws Put Virtually All Phones, Computers at Risk," January 04, 2018, Accessed January 31, 2018, https://www.reuters.com/article/us-cyber-intel/security-flaws-put-virtually-all-phones-computers-at-risk-idUSKBN1ES1BO.

Ms. Virginia M. Rometty February 15, 2018 Page 2 of 3

International Organization for Standardization (ISO).⁷ These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face.⁸ They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry's coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

- 1. When and how did you first become aware of these vulnerabilities?
- 2. Which of your products are affected by these vulnerabilities and how are they affected?
- 3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

⁷ Nat'l Inst. of Standards and Tech., Computer Security Resource Center, "Non-Invasive Attack Testing Workshop," Updated August 17, 2011, available at: https://csrc.nist.gov/Events/2011/Non-Invasive-Attack-Testing-Workshop; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/52906.html; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/60612.html

⁸ Schneier, Bruce, "The New Way Your Computer Can Be Attacked," *The Atlantic*, January 22, 2018, accessed February 01, 2018, https://www.theatlantic.com/technology/archive/2018/01/spectre-meltdown-cybersecurity/551147/.

⁹ Newman, Lily Hay, "Meltdown and Spectre Patching has been a Total Train Wreck," *Wired*, January 23, 2018, accessed February 1, 2018, https://www.wired.com/story/meltdown-spectre-patching-total-train-wreck/

¹⁰ McMillan, Robert, and Liza Lin, "Intel Warned Chinese Companies of Chip Flaws before U.S. Government," January 28, 2018, accessed February 1, 2018, https://www.wsj.com/articles/intel-warned-chinese-companies-of-chip-flaws-before-u-s-government-1517157430.

- 4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?
- 5. What steps have you taken to mitigate or patch these vulnerabilities?
- 6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?
- 7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.
- 8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?
- 9. To what degree are you coordinating your response with other companies?
- 10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

Sincerely,

JOHN THUNE

Chairman

Nelson Ranking Member

ROGER WICKER, MISSISSIPP
ROY BILLINT, MISSOURI
TED CRUZ, TEXAS
DEB FISCHER, NEBRASKA
JERRY MORRAN, KANSAS
DANS SULLIVANA, ALASKA
DEAN MELLER, NEVADA
JAMES INHOPE, OKLAHOMA
MIKE LEE, UTAH
ROM JOHNSON, WISCONSIN
SHELLEY MOORE CAPITO, WEST VIRGINIA
CORY GARDNER, COLORADO

BILL NELSON, FLORIDA
MARIA CANTIVELL, WASHINGTON
AMY KLOBUCHAR, MINNESOTA
RICHARD BLUMENTHAL, CONNECTICUT
BRIAN SCHATZ, HAWAII
EDWARD MARIKEV, MASSACHUSETTS
TOM UDALL, NEW MENICO
GARY PETERS, MICHIGIAN
TAMMY BALDWIN, WISCONSIN
TAMMY DUCKWORTH, BLINGIS
MAGGIE HASSTO, NEW HAMPSHIRE
CATHERINE CORTEZ MASTO, NEVADA

NICK ROSSI, STAFF DIRECTOR
KIM LIPSKY, DEMOCRATIC STAFF DIRECTOR

United States Senate

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEBSITE: http://commerce.senate.gov

February 15, 2018

Mr. Simon Segars Chief Executive Officer ARM Holdings PLC 150 Rose Orchard Way San Jose, CA 95134

Dear Mr. Segars:

Academic and independent security researchers,¹ some of whom were federally-funded,² recently discovered three vulnerabilities in modern computer processers that have existed for more than two decades.³ These side-channel vulnerabilities,⁴ which researchers have named "Meltdown" and "Spectre," could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information.⁵

According to one of the researchers, the Meltdown vulnerability is "probably one of the worst CPU [central processing unit] bugs ever found," while Spectre, although arguably more difficult to exploit, presents more significant challenges to mitigate or patch. For years, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has been concerned with such side-channel attacks and their impact on cryptography. In 2011, NIST held a testing workshop and coauthored standards in cooperation and accordance with the

¹ Affiliated with Google's Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.

² Nat'l Instl of Standards and Tech., "70NANB15H328, Provable Security for Next-Generation Cryptography;" Nat'l Sci. Found., "Award 1514261, TWC: Medium: Apollo: An Architecture for Scalable Verifiable Computing;" and Nat'l Sci. Found., "Award 1652259, CAREER: Towards Practical Systems for Trustworthy Cloud Computing." ³ Horn, Jann, "Reading Privileged Memory with a Side-Channel," January 3, 2018; Kocher, Paul, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom, "Spectre Attacks: Exploiting Speculative Execution," January 03, 2018; Lipp, Moritz, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg, "Meltdown," January 03, 2018; Galowicz, Jacek, Cyberus Technology, "Meltdown," January 3, 2018.

⁴ Nat'l Inst. of Standards and Tech., Nat'l Vulnerability Database, "CVE-2017-5754 Detail," "CVE-2017-5733 Detail," and "CVE-2017-5715 Detail," January 4, 2018.

⁵ "Alert (TA 1804A): Meltdown and Spectre Side-Channel Vulnerability Guidance," January 4, 2018, https://www.us-cert.gov/ncas/alerts/TA18-004A.

⁶ Busvine, Douglas, and Stephen Nellis, "Security Flaws Put Virtually All Phones, Computers at Risk," January 04, 2018, Accessed January 31, 2018, https://www.reuters.com/article/us-cyber-intel/security-flaws-put-virtually-all-phones-computers-at-risk-idUSKBN1ES1BO.

Mr. Simon Segars February 15, 2018 Page 2 of 3

International Organization for Standardization (ISO).⁷ These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face.⁸ They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry's coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

- 1. When and how did you first become aware of these vulnerabilities?
- 2. Which of your products are affected by these vulnerabilities and how are they affected?
- 3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

⁷ Nat'l Inst. of Standards and Tech., Computer Security Resource Center, "Non-Invasive Attack Testing Workshop," Updated August 17, 2011, available at: https://csrc.nist.gov/Events/2011/Non-Invasive-Attack-Testing-Workshop; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/52906.html; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/60612.html

8 Schneier, Bruce, "The New Way Your Computer Can Be Attacked," *The Atlantic*, January 22, 2018, accessed February 01, 2018, https://www.theatlantic.com/technology/archive/2018/01/spectre-meltdown-cybersecurity/551147/.

⁹ Newman, Lily Hay, "Meltdown and Spectre Patching has been a Total Train Wreck," *Wired*, January 23, 2018, accessed February 1, 2018, https://www.wired.com/story/meltdown-spectre-patching-total-train-wreck/

¹⁰ McMillan, Robert, and Liza Lin, "Intel Warned Chinese Companies of Chip Flaws before U.S. Government," January 28, 2018, accessed February 1, 2018, https://www.wsj.com/articles/intel-warned-chinese-companies-of-chip-flaws-before-u-s-government-1517157430

- 4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?
- 5. What steps have you taken to mitigate or patch these vulnerabilities?
- 6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?
- 7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.
- 8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?
- 9. To what degree are you coordinating your response with other companies?
- 10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

Sincerely,

JOHN THUNE

Chairman

BILL NELSON Ranking Member

L Nolson

ROGEN WICKER, MISSISSIPPI ROY BLUNT, MISSOURI TEO CHUZ, TEXAS DEB FISCHER, NEBRASKA JERRY MORAN, KANSAS DAN SULLIVAN, ALASKA DEAN HELLER, NEVADA JAMES INHOPE, OKLAHDMA MIKE LEE, UTAH RON JOHNSON, WISCONSIN SHELLEY MOORE CAPITO, WEST VIRGINIA CORY GARDNER, CILICORADO TODO VOLING, INDIANA

BILL NELSON, FLORIDA
MARIA CANTWELL, WASHINGTON
MARIA CANTWELL, WASHINGTON
AMY KLOBUCHAR MINNESOTA
RICHARD BLUMENTHAL, CONNECTICUT
BRIAN SCHATZ, HAWANI
EDWARD MARKEY, MASSACHUSETTS
TOM UDALL. NEW MEXICO
GARTY PETERS, MICHIGAN
TAMMY BALDWIN, WISCONSIN
TAMMY BUCKWORTH ILLINDIS
MAGGIE HASSAN, NEW HAMPSHIRE
CATHERINE CORTEZ MASTO, NEVADA
JON TESTER, MIGHTANA

NICK ROSSI, STAFF DIRECTOR KIM LIPSKY, DEMOCRATIC STAFF DIRECTOR

United States Senate

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEBSITE: http://commerce.senate.gov

February 15, 2018

Dr. Lisa Su President and Chief Executive Officer Advanced Micro Devices, Inc. 2485 Augustine Drive Santa Clara, CA 95054

Dear Dr. Su:

Academic and independent security researchers, ¹ some of whom were federally-funded, ² recently discovered three vulnerabilities in modern computer processers that have existed for more than two decades. ³ These side-channel vulnerabilities, ⁴ which researchers have named "Meltdown" and "Spectre," could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information. ⁵

¹ Affiliated with Google's Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.

² Nat'l Instl of Standards and Tech., "70NANB15H328, Provable Security for Next-Generation Cryptography;" Nat'l Sci. Found., "Award 1514261, TWC: Medium: Apollo: An Architecture for Scalable Verifiable Computing;" and Nat'l Sci. Found., "Award 1652259, CAREER: Towards Practical Systems for Trustworthy Cloud Computing." ³ Horn, Jann, "Reading Privileged Memory with a Side-Channel," January 3, 2018; Kocher, Paul, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom, "Spectre Attacks: Exploiting Speculative Execution," January 03, 2018; Lipp, Moritz, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg, "Meltdown," January 03, 2018; Galowicz, Jacek, Cyberus Technology, "Meltdown," January 3, 2018.

⁴ Nat'l Inst. of Standards and Tech., Nat'l Vulnerability Database, "CVE-2017-5754 Detail," "CVE-2017-5733 Detail," and "CVE-2017-5715 Detail," January 4, 2018.

⁵ "Alert (TA 1804A): Meltdown and Spectre Side-Channel Vulnerability Guidance," January 4, 2018, https://www.us-cert.gov/ncas/alerts/TA18-004A.

⁶ Busvine, Douglas, and Stephen Nellis, "Security Flaws Put Virtually All Phones, Computers at Risk," January 04, 2018, Accessed January 31, 2018, https://www.reuters.com/article/us-cyber-intel/security-flaws-put-virtually-all-phones-computers-at-risk-idUSKBN1ES1BO.

Dr. Lisa Su February 15, 2018 Page 2 of 3

International Organization for Standardization (ISO).⁷ These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face.⁸ They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry's coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

- 1. When and how did you first become aware of these vulnerabilities?
- 2. Which of your products are affected by these vulnerabilities and how are they affected?
- 3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

Nat'l Inst. of Standards and Tech., Computer Security Resource Center, "Non-Invasive Attack Testing Workshop," Updated August 17, 2011, available at: https://csrc.nist.gov/Events/2011/Non-Invasive-Attack-Testing-Workshop; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/52906.html; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/60612.html Schneier, Bruce, "The New Way Your Computer Can Be Attacked," *The Atlantic*, January 22, 2018, accessed February 01, 2018, https://www.theatlantic.com/technology/archive/2018/01/spectre-meltdown-cybersecurity/551147/.

⁹ Newman, Lily Hay, "Meltdown and Spectre Patching has been a Total Train Wreck," Wired, January 23, 2018, accessed February 1, 2018, https://www.wired.com/story/meltdown-spectre-patching-total-train-wreck/
¹⁰ McMillan, Robert, and Liza Lin, "Intel Warned Chinese Companies of Chip Flaws before U.S. Government," January 28, 2018, accessed February 1, 2018, https://www.wsj.com/articles/intel-warned-chinese-companies-of-chip-flaws-before-u-s-government-1517157430

- 4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?
- 5. What steps have you taken to mitigate or patch these vulnerabilities?
- 6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?
- 7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.
- 8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?
- 9. To what degree are you coordinating your response with other companies?
- 10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

Sincerely,

JOHN THUNE Chairman

Ranking Member

L Nelson

RÜĞER WICKER, MISSISSIPPI ROV BUNT, MISSOURI TED CRUZ, TEXAS DEB FISCHER, NEBRASIKA JERRY MÜRAN, KANSAS JAN SULLIVAN, ALASKA DEAN HELLER, NEVADA JAMES INHOEF, GIKLAHOMA MIKE LEE, UTAH RICH JOHNSON, WISCONBIN SHELLEY MOORE CAPITO, WEST VIRGINIA CURY GARDINER, COLORADO CORN CONTROL MISSON BILL NELSON, FLORIDA
MARIA CANTWELL, WASHINGTON
AMY KLOBUCHAR, MINNESOTA
RICHARD BILUMENTHAL, CONNECTICUT
BIRAN SCHAETZ, PARWAIT
FOWARD MARKEY, MASSACHUSETTS
TOM UDALL, NEW MEXICO
GARY PETERS, MICHIGAN
TAMMY BALDWIN, WISCONSIN
TAMMY BULCKWORTH, ILLINOIS
MAGGIE HASSAN, NEW HAMPSHIRE
CA THERINE CORTEZ MASTO, NEVADA
JON TESTER, MONTANA

NICK ROSSI, STAFF DIRECTOR
KIM LIPSKY, DEMOCRATIC STAFF DIRECTOR

United States Senate

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEBSITE: http://commerce.senate.gov

February 15, 2018

Mr. Yang Yuanqing Chairman and Chief Executive Officer Lenovo Group Limited 1009 Think Place Morrisville, NC 27560

Dear Mr. Yuanqing:

Academic and independent security researchers, some of whom were federally-funded, recently discovered three vulnerabilities in modern computer processers that have existed for more than two decades. These side-channel vulnerabilities, which researchers have named "Meltdown" and "Spectre," could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information.

According to one of the researchers, the Meltdown vulnerability is "probably one of the worst CPU [central processing unit] bugs ever found," while Spectre, although arguably more difficult to exploit, presents more significant challenges to mitigate or patch. For years, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has been concerned with such side-channel attacks and their impact on cryptography. In 2011, NIST held a testing workshop and coauthored standards in cooperation and accordance with the

¹ Affiliated with Google's Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.

² Nat'l Instl of Standards and Tech., "70NANB15H328, Provable Security for Next-Generation Cryptography;" Nat'l Sci. Found., "Award 1514261, TWC: Medium: Apollo: An Architecture for Scalable Verifiable Computing;" and Nat'l Sci. Found., "Award 1652259, CAREER: Towards Practical Systems for Trustworthy Cloud Computing." ³ Horn, Jann, "Reading Privileged Memory with a Side-Channel," January 3, 2018; Kocher, Paul, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom, "Spectre Attacks: Exploiting Speculative Execution," January 03, 2018; Lipp, Moritz, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg, "Meltdown," January 03, 2018; Galowicz, Jacek, Cyberus Technology, "Meltdown," January 3, 2018.

⁴ Nat'l Inst. of Standards and Tech., Nat'l Vulnerability Database, "CVE-2017-5754 Detail," "CVE-2017-5733 Detail," and "CVE-2017-5715 Detail," January 4, 2018.

⁵ "Alert (TA 1804A): Meltdown and Spectre Side-Channel Vulnerability Guidance," January 4, 2018, https://www.us-cert.gov/ncas/alerts/TA18-004A.

⁶ Busvine, Douglas, and Stephen Nellis, "Security Flaws Put Virtually All Phones, Computers at Risk," January 04, 2018, Accessed January 31, 2018, https://www.reuters.com/article/us-cyber-intel/security-flaws-put-virtually-all-phones-computers-at-risk-idUSKBN1ES1BO.

Mr. Yang Yuanqing February 15, 2018 Page 2 of 3

International Organization for Standardization (ISO).⁷ These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face.⁸ They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry's coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

- 1. When and how did you first become aware of these vulnerabilities?
- 2. Which of your products are affected by these vulnerabilities and how are they affected?
- 3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

Nat'l Inst. of Standards and Tech., Computer Security Resource Center, "Non-Invasive Attack Testing Workshop," Updated August 17, 2011, available at: https://csrc.nist.gov/Events/2011/Non-Invasive-Attack-Testing-Workshop; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/52906.html; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology – Security Techniques – Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/60612.html
Schneier, Bruce, "The New Way Your Computer Can Be Attacked," The Atlantic, January 22, 2018, accessed February 01, 2018, https://www.theatlantic.com/technology/archive/2018/01/spectre-meltdown-cybersecurity/551147/.

⁹ Newman, Lily Hay, "Meltdown and Spectre Patching has been a Total Train Wreck," *Wired*, January 23, 2018, accessed February 1, 2018, https://www.wired.com/story/meltdown-spectre-patching-total-train-wreck/

¹⁰ McMillan, Robert, and Liza Lin, "Intel Warned Chinese Companies of Chip Flaws before U.S. Government," January 28, 2018, accessed February 1, 2018, https://www.wsj.com/articles/intel-warned-chinese-companies-of-chip-flaws-before-u-s-government-1517157430

- 4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?
- 5. What steps have you taken to mitigate or patch these vulnerabilities?
- 6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?
- 7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.
- 8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?
- 9. To what degree are you coordinating your response with other companies?
- 10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

Sincerely,

JOHN THUNE

Chairman

BILL NELSON Ranking Member

L Nelson

ROGER WICKER, MISSISSIPP ROY BLUNT, MISSOURI TED CRUZ, EXAS DEB FISCHER, NEBBASKA JERRY MODRAN KANSAS DAN SULLIVAN, ALASKA DEAN HELLER, NEVADA JAMES INHOPE. OKLAHOMA MIKE LEF, UTAH ROW, JOHNSON, WISCONSIN SHELLEY MOORE CAPITO, WEST VIRGINIA CORY GARDNER, COLGRADO BILL NELSON, FLORIDA
MARIA CANTIVELL, WASHINGTON
AMY KLOBUCHAR, MINNESDTA
RICHARD BLUMENTHAL CONNECTICUT
BRILAN SCHATZ, HAWAII
EDWARD MARKEY, MASSACHUSE ITS
TOM UDALL. NEW MEXICO
GARY RETERS, MICHIGAN
TAMMY BALDWIN, WISCONSIN
TAMMY DUCKWORTH, LLINDIS
MAGGIE HASSAN, NEW HAMPSHIRE
CATHERINE CORTEZ MASTO, NEVADA
WIN TEXTERN

NICK ROSSI, STAFF DIRECTOR
KIM LIPSKY, DEMOCRATIC STAFF DIRECTOR

United States Senate

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEBSITE: http://commerce.senate.gov

February 15, 2018

Mr. Ren Zhengfei Deputy Chairman of the Board and Chief Executive Officer Huawei Technologies, Co., Ltd. c/o Huawei Technologies USA 5700 Tennyson Parkway Suite 500 Plano, TX 75024

Dear Mr. Zhengfei:

Academic and independent security researchers, 1 some of whom were federally-funded, 2 recently discovered three vulnerabilities in modern computer processers that have existed for more than two decades. 3 These side-channel vulnerabilities, 4 which researchers have named "Meltdown" and "Spectre," could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information. 5

¹ Affiliated with Google's Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.

² Nat'l Instl of Standards and Tech., "70NANB15H328, Provable Security for Next-Generation Cryptography;" Nat'l Sci. Found., "Award 1514261, TWC: Medium: Apollo: An Architecture for Scalable Verifiable Computing;" and Nat'l Sci. Found., "Award 1652259, CAREER: Towards Practical Systems for Trustworthy Cloud Computing." ³ Horn, Jann, "Reading Privileged Memory with a Side-Channel," January 3, 2018; Kocher, Paul, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom, "Spectre Attacks: Exploiting Speculative Execution," January 03, 2018; Lipp, Moritz, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg, "Meltdown," January 03, 2018; Galowicz, Jacek, Cyberus Technology, "Meltdown," January 3, 2018.

⁴ Nat'l Inst. of Standards and Tech., Nat'l Vulnerability Database, "CVE-2017-5754 Detail," "CVE-2017-5733 Detail," and "CVE-2017-5715 Detail," January 4, 2018.

⁵ "Alert (TA 1804A): Meltdown and Spectre Side-Channel Vulnerability Guidance," January 4, 2018, https://www.us-cert.gov/ncas/alerts/TA18-004A.

⁶ Busvine, Douglas, and Stephen Nellis, "Security Flaws Put Virtually All Phones, Computers at Risk," January 04, 2018, Accessed January 31, 2018, https://www.reuters.com/article/us-cyber-intel/security-flaws-put-virtually-all-phones-computers-at-risk-idUSKBN1ES1BO.

Mr. Ren Zhengfei February 15, 2018 Page 2 of 3

International Organization for Standardization (ISO).⁷ These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face.⁸ They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry's coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

- 1. When and how did you first become aware of these vulnerabilities?
- 2. Which of your products are affected by these vulnerabilities and how are they affected?
- 3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

⁷ Nat'l Inst. of Standards and Tech., Computer Security Resource Center, "Non-Invasive Attack Testing Workshop," Updated August 17, 2011, available at: https://csrc.nist.gov/Events/2011/Non-Invasive-Attack-Testing-Workshop; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology — Security Techniques — Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/52906.html; International Organization for Standardization, "ISO/IEC 17825:2016: Information Technology — Security Techniques — Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules," January 2016, https://www.iso.org/standard/60612.html
⁸ Schneier, Bruce, "The New Way Your Computer Can Be Attacked," *The Atlantic*, January 22, 2018, accessed February 01, 2018, https://www.theatlantic.com/technology/archive/2018/01/spectre-meltdown-cybersecurity/551147/.

⁹ Newman, Lily Hay, "Meltdown and Spectre Patching has been a Total Train Wreck," Wired, January 23, 2018, accessed February 1, 2018, https://www.wired.com/story/meltdown-spectre-patching-total-train-wreck/

¹⁰ McMillan, Robert, and Liza Lin, "Intel Warned Chinese Companies of Chip Flaws before U.S. Government," January 28, 2018, accessed February 1, 2018, https://www.wsj.com/articles/intel-warned-chinese-companies-of-chip-flaws-before-u-s-government-1517157430

- 4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?
- 5. What steps have you taken to mitigate or patch these vulnerabilities?
- 6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?
- 7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.
- 8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?
- 9. To what degree are you coordinating your response with other companies?
- 10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

Sincerely,

JOHN THUNE Chairman Bill Nelson Ranking Member